AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. A secure processing unit, the secure processing unit including:

   an internal memory unit;

   a processor;

   tamper detection and response logic;

   an interface to external systems or components;

   one or more buses for connecting the internal memory unit, the processor, the tamper detection and response logic, and the interface to external systems and components; and

   a tamper-resistant housing.

2. A secure processing unit as in claim 1, in which the internal memory unit includes:

   secure random access memory;

   secure non-volatile memory;

   secure read-only memory.

3. A secure processing unit as in claim 2, in which the secure non-volatile memory is powered by a battery.

4. A secure processing unit as in claim 3, in which the secure non-volatile memory contains at least one cryptographic key.

5. A secure processing unit as in claim 1, in which the internal memory unit includes a unique identifier for the secure processing unit, a private cryptographic key, a public cryptographic key, and a cryptographic certificate linking the unique identifier and the public cryptographic key.

6. A secure processing unit as in claim 1, in which the processor includes:

a memory management unit; and

a plurality of processor security registers.

7. A secure processing unit as in claim 6, including:

access control data, the access control data being operable to indicate whether access to predefined memory regions is restricted to certain software components or processor modes.

8. A secure processing unit as in claim 7, in which the access control data are stored in a critical address register, the critical address register comprising one of the processor security registers.

9. A secure processing unit as in claim 6, the secure processing unit further including a level-one page table, the level-one page table including a plurality of level-one page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit whether entries in a corresponding level-two page table may designate certain predefined memory regions.

10. A secure processing unit as in claim 9, whereby level-two page tables that may not designate the predefined memory regions are not stored in the internal memory unit.

11. An information appliance, the information appliance comprising:

a memory unit;

a secure processing unit, the secure processing unit including:

a tamper resistant packaging;

tamper detection and response logic;

a secure memory unit;

a processing unit, including a memory management unit and a plurality of processor security registers;

a bus for connecting the memory unit and the secure processing unit;

wherein the secure processing unit is operable to perform both secure processing operations and at least some processing operations performed by a conventional information appliance processing unit.

12. An information appliance as in claim 11, in which the information appliance is selected from the group comprising: a television set-top box, a portable audio player, a portable video player, a cellular telephone, a personal computer, and a workstation.

13. An information appliance as in claim 11, in which the secure processing unit is the information appliance's primary processing unit.

14. An information appliance as in claim 11, in which the secure processing unit is the information appliance's only processing unit.

15. An information appliance as in claim 11, in which the secure processing unit includes:

a critical address register, the critical address register containing a plurality of access control bits, the access control bits being operable to indicate whether access to associated memory regions is restricted to predefined software components or processor modes.

16. An information appliance as in claim 15, in which the critical address register comprises one of the processor security registers.

17. An information appliance as in claim 11, further including:

a level-one page table and a plurality of level-two page tables, the level-one page table including a plurality of level-one page table entries and the level-two page table including a plurality of level-two page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit whether a corresponding level-two page table may designate certain predefined memory regions.

18. An information appliance as in claim 17, in which level-two page tables that may not designate the predefined memory regions are stored in the memory unit, and wherein the level-one page table and the level-two page tables that may designate the predefined memory regions are stored in the secure memory unit.

19.-21. (Canceled)